UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/567,752	02/10/2006	Paolo Abeni	09952.0022	5634

22852 7590 01/05/2011
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER
SIMS, JING F

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
01/05/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/567,752	**Applicant(s)** ABENI, PAOLO	
	Examiner Jing Sims	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2010*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *26-50* is/are pending in the application.

4a) Of the above claim(s) *1-25* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *26-50* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communications filed on 10/25/2010 with application 11/567,752.

2. Claims 26 and 38 are amended.

3. The 35 U.S.C. §112 rejection over claim 26 is withdrawn in view of Applicant's amendments.

Response to Arguments

4. Applicant's arguments with respect to claims 26 and 38 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. **Claims 26, 27, 29, 38, 39, 41 and 50 are rejected under 35 U.S.C. 102(e) as being anticipated by Tarquini et al. (US 2003/0101353 A1, hereinafter, Tarquini)**.

Tarquini discloses:

As per claim 26, **an intrusion detection system**, **for detecting unauthorised use of a network** (e.g., [0027]: a network based Intrusion Prevention System, IPS), comprising:

at least one computer (e.g., [0035]: an IPS server run an instance of an IPS application; see also Fig. 4);

a database storing attack signatures and, for each of the attack signatures, a set of at least one corresponding response signature (e.g., [0027]: a database 80A and 81A of known attack signature, or rules, against which network frames captured thereby may be compared); and

a non-transitory computer readable medium encoded with a computer program product loadable into a memory of the at least one computer (e.g., [0035]: database 277 that is loadable into memory module 274 and maybe retrieved by IPS application 91 for analysis of network frames and/or packets), the computer program product including:

instructions for a sniffer for capturing data being transmitted on said network (e.g., [0048]: perform signature matching on network frames),

instructions for a pattern matching engine for comparing the captured data with the attack signatures for generating an event when a match between the captured data and at least one attack signature is found (e.g., [0048]: the event corresponding to the action of having signature files passed thereto that may comprise machine-readable code representative of an inbound signature of a reconnaissance probe and having the inbound reconnaissance probe signature maintained in a signature file), and

instructions for a response analysis engine triggered by said event (e.g., [0048]: a subsequent detection of an outbound response signature generated by the probed network stack in response to the probe packet and/or frame may allow the IPS to affirmatively evaluate the probe packet and/or frame as a reconnaissance attack; an inbound reconnaissance probe signature maintained in a signature file and a correspondence between an analyzed signature of the response packet generated by network stack and an outbound response signature maintained in the signature file may invoke network filter service provider 140 to perform a directive maintained in the signature file), **for selecting**, **from the database**, **a selected set of at least one response signature corresponding to the at least one matched attack signature** (e.g., [0048]: the outbound response signature corresponding with response signature; the network filter service provider may perform a signature analysis on response packet and identify reconnaissance probe attack; see also abstract regarding the section of determining the second signature), **and comparing**, **with the selected set of at least one response signature** (e.g., [0048]: perform a signature analysis on response packet), **response data being transmitted on said network as a response to said captured data and for correlating results of said comparisons with attack and response signatures for generating an alarm** (e.g., [0048]: an outbound response signature maintained in the signature file may invoke network filter service provider to perform a directive maintained in the signature file, such as logging of the identified reconnaissance probe, discarding of the response packet and/or execution of another security measure).

As per claim 27, the system of claim 26 is incorporated, and wherein said response data is captured by said sniffer by performing an analysis of source IP address in data packets transmitted on said network *(e.g., [0038], IP port filtering)*.

As per claim 29, the system of claim 26, wherein said response data is captured by said sniffer by analysing transport level information in data packets transmitted on said network *(e.g., [0040]: provide network exploit detection at the transport layer lever)*;

As per claim 38, **a method performed using one or more computers for detecting unauthorised use of a network** (e.g., [0027]: a network based Intrusion Prevention System, IPS), comprising:

capturing data, **using the one or more computers**, **being transmitted on said network** (e.g., [0048]: perform signature matching on network frames);

comparing the captured data with attack signatures for generating an event, **using the one o more computers**, **when a match between the captured data and at least one attack signature is found** (e.g., [0048]: the event corresponding to the action of having signature files passed thereto that may comprise machine-readable code representative of an inbound signature of a reconnaissance probe and having the inbound reconnaissance probe signature maintained in a signature file); and

when triggered by said event (e.g., [0048]: a subsequent detection of an outbound response signature generated by the probed network stack in response to the probe packet and/or frame may allow the IPS to affirmatively evaluate the probe packet and/or frame as a reconnaissance attack; an inbound reconnaissance probe signature maintained in a signature file and a correspondence between an analyzed signature of the response packet generated by network stack and an outbound response signature maintained in the signature file may invoke network filter service provider 140 to perform a directive maintained in the signature file),:

selecting, **from a database**, **a selected set of at least one response signature corresponding to the at least one matched attack signature** (e.g., [0048]: the outbound response signature corresponding with response signature; the network filter service provider may perform a signature analysis on response packet and identify reconnaissance probe attack; see also abstract regarding the section of determining the second signature);

comparing with the selected set of at least one response signature signatures (e.g., [0048]: perform a signature analysis on response packet), using the one or more computers, **response data being transmitted on said network as a response to said captured data matched with said at least one attack signature alarm** (e.g., [0048]: an outbound response signature maintained in the signature file may invoke network filter service provider to perform a directive maintained in the signature file, such as logging of the identified reconnaissance probe, discarding of the response packet and/or execution of another security measure); and

correlating results of said comparisons, using the one or more computers, with attack and response signatures for generating an alarm (e.g., [0048]: an outbound response signature maintained in the signature file may invoke network filter service provider to perform a directive maintained in the signature file, such as logging of the identified reconnaissance probe, discarding of the response packet and/or execution of another security measure).

Claims 39 and 41 are method claims corresponding to the system claims 27, and 29 therefore are rejected under the same reasons set forth in the rejections for claims 27, and 29.

As per claim 50, a non-transitory computer readable medium encoded with a computer program product loadable into a memory of at least one computer, the computer program product including software code portions for performing the method of any one of claims 38 to 49 *(e.g., [0035]: database 277 that is loadable into memory module 274 and maybe retrieved by IPS application 91 for analysis of network frames and/or packets; see also Fig. 4).*

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 28 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini in view of Lahtinen (European Publication no. EP 1330095 A1)**.

As per claim 28, the system of claim 26 is incorporated and Tarquini discloses analyzing captured data by applying IP port filtering; however, Tarquini does not performing an analysis of both source and destination IP addresses in data packets transmitted on said network.

Lahtinen discloses wherein said response data is captured by said sniffer by performing an analysis of both source and destination IP addresses in data packets transmitted on said network *(e.g., page 3, [0009], IP frame on TCP packets, target and destination port, for example)*.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the IP filtering analysis that as described by Tarquini and add performing the analysis of both source and destination IP address in data packets as taught by Lahtinen because it would enhance security of the network.

Claim 40 is method claim corresponding to the system claim 28; therefore are rejected under the same reasons set forth in the rejections for claim 28.

9. **Claims 30 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini in view of Goldstone (US 7,301,899 B2)**.

As per claim 30, Tarquini discloses the system of claim 26 which alarming when there is possible attack, however, Tarquini does not disclose said response analysis engine generates the alarm when said response data indicates that a new network connection has been established.

Goldstone discloses wherein said response analysis engine generates the alarm when said response data indicates that a new network connection has been established *(e.g., col. 2, lines 58-60)*.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify generating information reporting an possible attack as described by Tarquini and add detecting a new connection as alarming situation as taught by Goldstone because it would provide positive steps in preventing or at least diminishing the potentially devastating effects of a DOS attack (see Goldstone, col. 4, lines 13-15).

Claim 42 is method claim corresponding to the system claim 30, therefore are rejected under the same reasons set forth in the rejections for claim 30.

10. **Claims 31-32 and 43-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini, in view of Cole et al. (US 2004/0015728 A1, hereinafter Cole)**.

As per claim 31, Tarquini discloses the system of claim 26 which including a response signatures, however, Tarquini does not specifically disclose wherein said response signatures are arranged in two categories, response signatures identifying an illicit traffic, and response signatures identifying legitimate traffic.

Cole discloses wherein said response signatures are arranged in two categories, response signatures identifying an illicit traffic, and response signatures identifying legitimate traffic *(e.g., [0361], high risk vulnerability level scale corresponding with illicit traffic, and low risk vulnerability level scale corresponding with legitimate traffic)*.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the response signature as described by Tarquini and add what the level categories are as taught by Cole because it would provide traditional vulnerability scale which easy and reasonable categorizing the risk levels (see Cole, [0360]).

As per claim 32, the system of claim 31 is incorporated, and Tarquini discloses:

wherein said response analysis engine generates the alarm when a match between the response_data and a response signature identifying illicit traffic is found *(e.g., [0048]: the outbound response signature corresponding with response signature; the network filter service provider may perform a signature analysis on response packet and identify reconnaissance probe attack; see also abstract regarding the section of determining the second signature)*.

Claim 43 and 44 are method claims corresponding to the system claims 31 and 32, therefore are rejected under the same reasons set forth in the rejections for claims 31 and 32.

11. **Claims 33, 34, 45, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini, in view of Cole, and further in view of Moharram (US 7,246,376 B2)**.

As per claim 33, Tarquini in view of Cole discloses the system of claim 31;

Tarquini and Cole do not disclose said response analysis engine comprises a counter which is incremented when a match between the response data and a response signature identifying legitimate traffic is found;

Moharram discloses a counter which is incremented when a match between the response data and a response signature identifying legitimate traffic is found *(e.g., col. 4, lines 13-16; and col. 5, claim 1, lines 48-53)*.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network filter service provider 140 as described by Tarquini and add a counter as taught by Maher because it would provide possibility of fine control over an objective subject.

As per claim 34, Moharram discloses when said counter reaches a predetermined value, said response analysis engine terminates without generating any alarm *(e.g., col. 5, claim 1)*.

Claims 45 and 46 are method claims corresponding to the system claims 33, and 34, therefore are rejected under the same reasons set forth in the rejections for claims 33 and 34.

12. **Claims 35-37 and 47-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini, in view of Moharram (US 7,246,376 B2)**.

As per claim 35, Tarquini discloses the system of claim 26. They do not disclose wherein said response analysis engine comprises a time-out system triggered by said event for starting a probing task.

Moharram discloses wherein said response analysis engine comprises a time-out system triggered by said event for starting a probing task *(e.g., col. 5, claim 1, see also Fig. 3, lines 5-35)*.

As per claim 36, the system of claim 35 is incorporated.

Moharram discloses:

wherein said probing task verifies if any data has been detected on said network as the response to said data matched with said at least one attack signature and, if such condition is verified:

generates the alarm in case only response signatures indicating legitimate traffic have been used by said response analysis engine *(e.g., col. 5, claim 1, lines 48-53)*; or

ends the probing task in case only response signatures indicating illicit traffic or both response signatures indicating legitimate traffic and illicit traffic have been used by said response analysis engine *(e.g., col. 5, claim 1)*.

As per claim 37, the system of claim 36 is incorporated, and Tarquini discloses:

wherein, if such condition is not verified, said probing task attempts to perform a connection to a suspected attacked computer, for generating the alarm if such attempt is successful, or for ending the probing task if such attempt is unsuccessful *(e.g., [0048])*.

Claim 47-49 are method claims corresponding to the system claims 35-37, therefore are rejected under the same reasons set forth in the rejections for claims 35-37.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jing Sims whose telephone number is (571)270-7315. The examiner can normally be reached on 9:00am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. S./
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437